UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/972,371	10/05/2001	Ryuichi Iwamura	SONY-50R4813	4728

7590 09/18/2007

WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose, CA 95113

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
09/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/972,371
Filing Date: October 05, 2001
Appellant(s): IWAMURA, RYUICHI

Anthony C. Murabito
Reg No. 35,295
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 29 May 2007 appealing from the Office action mailed 25 January 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,373,946	JOHNSTON	4-2002
6,055,314	SPIES	4-2000
5,721,781	DEO	2-1998

Waktinson, John, The MPEG Handbook, Focal Press, Second Edition, 2004, pp 366-381, 389-394.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 17-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Johnston, U.S. Patent No. 6,373,946. Referring to claim 17, Johnston discloses a communication security system wherein a mobile handset terminal (Figure 2) comprises a terminal processor (Figure 2, element 37) and a SIM card (Figure 2, element 35). The mobile handset terminal meets the limitation of the digital media receiving device. The SIM card meets the limitation of a first logical circuit, and the terminal processor meets the limitation of the second logical circuit. The SIM card receives a partial key that is used to generate an encryption key (Col. 10, lines 36-43, 52-53 & Col. 11, lines 14-17). The SIM card supplies this encryption key to the terminal processor to encrypt data (Col. 10, lines 51-53), which meets the limitation of a second logical circuit for encrypting said digital signal using said local encryption key accessed from said first logical circuit. Prior to transmitting the encryption key to the terminal processor, the SIM card decrypts the partial key that is ultimately used to generate the encryption key (Col. 12, lines 20-24), which meets the limitation of a first logical circuit for decrypting a local encryption key. The SIM card contains a processor (Figure 2, element 35a) and a memory (Figure 2, element 35b & Col. 6, lines 20-23), which meets the limitation of said first logical circuit comprising a local processor and local memory.

Referring to claim 18, Johnston discloses that the SIM card stores an encryption algorithm to decrypt data (Col. 12, lines 8-12), which meets the limitation of a computer control

program contained within said first logical circuit, said computer control program for controlling said local processor and for receiving said encryption key in an encrypted form and for decrypting said encryption key prior to providing said encryption key to said second logical circuit.

Referring to claim 19, Johnston discloses that the SIM cards are reprogrammable so that they may be tailored so specific communication environments (Col. 16, lines 47-49), which meets the limitation of a modifiable local memory contained within said first logical circuit, said modifiable local memory enabling the modification of a computer control program stored within said local memory.

Referring to claim 20, Johnston discloses that the data stored in the SIM cannot be read or accessed (Col. 1, lines 36-37), which meets the limitation of the contents of said local memory cannot be observed from outside of said first logical circuit.

Claims 1, 3-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies, U.S. Patent No. 6,055,314, in view of Deo, U.S. Patent No. 5,721,781. Referring to claim 1, Spies discloses a secure video content delivery system wherein an IC card contains public/private key pairs (Figure 6 & Col. 11, lines 40-42), which meets the limitation of generating a public encryption key. The IC card contains functionality to perform key management, encryption/decryption, hashing, digital signing, and authentication (Col. 11, lines 50-55). Encrypted video data is received at the set top box (Figure 7) and passed to the processor of the set top box, along with the decryption key from the IC card, to facilitate decryption of the video data (Col. 12, line 61 – Col. 13, line 10), which meets the limitation of in a digital media receiving device, accessing an encrypted signal at said first logical circuit, determining a first

decryption key for said encrypted signal at said logical circuit, at said first logical circuit decrypting said encrypted signal using said first decryption key. Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted decryption key can only be decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Referring to claim 3, Spies the IC card contains public/private key pairs (Figure 6 & Col. 11, lines 40-42), which meets the limitation of accessing said public encryption key from a first portion of local memory at said second logical circuit. The IC card contains functionality to perform key management, encryption/decryption, hashing, digital signing, and authentication (Col. 11, lines 50-55), which meets the limitation of accessing a computer control program for a second portion of local of local memory at said second logical circuit. Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key

so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted decryption key can only be decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Referring to claims 4, 5, Spies the IC card contains public/private key pairs (Figure 6 & Col. 11, lines 40-42), which meets the limitation of accessing said public encryption key from a first portion of local memory at said second logical circuit. The IC card contains functionality to perform key management, encryption/decryption, hashing, digital signing, and authentication (Col. 11, lines 50-55). The IC card functionality can be updated or changed (Col. 12, lines 1-4). which meets the limitation of replacing a computer control program stored in a second portion of local memory at said second logical circuit with a new computer control program, accessing said new computer control program from said second portion of local memory. Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted

decryption key can only be decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Referring to claim 6, Spies discloses that the cryptographic functions can be updated by replacing DLLs (Col. 12, lines 1-4), which meets the limitation of accessing a second decryption key from a first portion of local memory at said first logical circuit, replacing a computer control program stored in a second portion of local memory at least first logical circuit with a new computer control program, accessing said new computer control program from said second portion of local memory, and executing said new computer control program at said second logical circuit to decrypt said first decryption key using said second decryption key.

Referring to claim 7, Spies discloses that the video content can be TV broadcasts (Col. 1, lines 14-29), which are transmitted in MPEG format.

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Spies, U.S. Patent No. 6,055,314, in view of Deo, U.S. Patent No. 5,721,781 as applied to claim 1 above, and further in view of Schneier. Referring to claim 2, Spies does not disclose using Diffie-Hellman algorithm for key exchange. Schneier discloses using the Diffie-Hellman algorithm for public key exchange (Pages 513-514). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the Diffie-Hellman algorithm for public key exchange in the secure video content delivery system of Spies because Diffie-Hellman gets its security from the difficulty of calculating discrete logarithms in a finite field as taught by Schneier (Page 513).

(10) Response to Argument

Appellant argues, "that one of ordinary skill in the art would not understand the taught voice-only system of Johnston to teach or suggest 'digital media' as recited by Claim 17." This

argument is not persuasive because the voice communications over the system are in a digital format (Col. 1, line 13), and voice communications are a form of audio, which would be considered media using a broad but reasonable interpretation of "digital media".

Appellant argues, "that one of ordinary skill in the art would not understand the taught telephone to be a 'receiving' device. For example, transmission is fundamental to the operation of such a telephone. Appellants respectfully assert that one of ordinary skill in the art would understand the recited receiving device to be a device that primarily functions to receive. In contrast, the taught telephone has a primary function of two-way communication." This argument is not persuasive because if the taught telephone of Johnston "has a primary function of two-way communication", then the taught telephone can be considered a "receiving" device merely for the fact that the telephone of Johnston does in fact receive digital audio (as discussed above). Therefore, since the taught telephone of Johnston receives digital audio, it can be considered a "receiving" device using a broad but reasonable interpretation of the claims. Additionally, the Examiner respectfully points out that the claims are silent with respect to the transmission capabilities, or lack thereof, of the claimed device.

Appellant argues, "While Johnston may teach encrypting, such encrypting is taught 'for data to be transmitted' (column 10, line 53 *inter alia*, emphasis added). Johnston fails to teach of suggest encrypting data on reception as claimed." This argument is not persuasive because the claims do not require "encrypting data on reception" as alleged by Appellant. Claim 17 requires "a second logical circuit for encrypting said digital signal using said local encrypting key accessed from said first logical circuit." No mention is made in the claims as to the source of the digital signal, merely that it is encrypted. Therefore, Johnston meets the above mentioned claim

limitation merely for the fact that Johnston discloses encryption of data within the mobile phone (Col. 10, lines 51-53) regardless of whether the encrypted data is being transmitted from the phone.

Appellant argues, "Johnston actually teaches decryption of a received signal (column 11, lines 4-5), in contrast to embodiments in accordance with Claim 17 that recite encryption of a received signal. In this manner, Johnston actually teaches away from embodiments in accordance with the present invention as recited by Claim 17." This argument is not persuasive because, as stated above, the claims do not require "encryption of a received signal" as alleged by Applicant. The fact that Johnston decrypts received signals has no bearing on how Johnston meets the limitations of claim 17. The claim limitation in question is met since Johnston discloses encryption of data within the mobile phone (Col. 10, lines 51-53).

Appellant argues, "Johnston fails to teach or suggest the claimed limitation, 'a modifiable local memory contained within said first logical circuit, said modifiable local memory enabling the modification of a computer control program stored within said local memory...the rejection cites Johnston column 16 lines 47-49 as suggesting the limitations of this Claim...Neither the cited passage nor the whole of Johnston suggests modification of a SIM card, Johnston fails to suggest that such modifications take place within said 'digital media receiving device,' as recited by Claim 19." This argument is not persuasive because the claims do not require the memory to actually be **modified**. The claims only require that the memory is **modifiable**, meaning that it could be modified. Column 16, lines 47-49 of Johnston discusses that the SIM cards used the mobile phones are **reprogrammed**, meaning that they have been modified and would therefore meet the claim limitations because the SIM cards are clearly **modifiable** if they have in fact been

reprogrammed (i.e. modified by reprogramming). Therefore, the claims also do not require the memory to be modified within the claimed 'digital media receiving device' as alleged by Appellant for the same reasons stated above.

Appellant argues, "Deo teaches an authentication system that is dependent upon hardware comprising global secrets, e.g. digital certificates (Abstract). In contrast, Spies specifically teaches away from such a system. 'It is therefore another object of this invention to provide a...system that has no global secrets built into any hardware...' (Spies, column 2, lines 1-5). Consequently, Appellants respectfully assert that one of ordinary skill in the art would be taught away from the proposed modification of Spies in view of Deo in view of the teachings of Spies." This argument is not persuasive because Deo does not teach "an authentication system that is dependent upon hardware comprising global secrets, e.g. digital certificates" as alleged by Appellant. Careful study of Deo reference yields no recitation of "global secrets" as alleged by Appellant. Deo does in fact use digital certificates, but the digital certificates are public key certificates as evidenced by the Abstract, "The smart card is assigned its own digital certificate which contains a digital signature from a trusted certifying authority and a unique public key." Additionally, on column 7, lines 1-5, Deo discusses that "the smart card uses the terminal's public key that is received in the terminal's certificate to send a message." Once again, these digital certificates are public key certificates, and public certificates could never be confused with "global secrets", because by definition they are **public**. The private key of the terminal (discussed in Deo on Column 7, lines 1-5) could be considered a secret, but not a "global secret" as alleged by Appellant, since the private key is relegated to the terminal.

The portions of Spies (column 2, lines 1-5) relied upon by Appellant in the arguments is part of a larger discussion (Col. 1, line 37 – Col. 2, line 15) that details the desire of Spies to overcome the ability of pirates tamper with a settop box to reveal the security protocols (i.e. keys used to decrypt the video content) utilized in the settop box. The portion of Spies directly cited by Appellant (Col. 2, lines 1-5), discusses the desire of Spies to remove these decryption keys from the hardware of the settop box and is not relevant to providing the settop box with a public/private key pair as suggested by the combination of references.

In response to appellant's argument that the proposed combination would change the principle operation of at least one of the references (Pages 15-17 of the Appeal Brief), the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). The modification is **only** to encrypt the decryption key in the IC card, with the public key of the set top box, prior to transmitting the decryption key to the set top box. One of ordinary skill in the art at the time the invention was made would have been motivated to make such a modification so that the decryption key can only be accessed (decrypted in this case) by the set top box (using the set top box specific private key) in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Appellant argues, "that the rejection's citation of Deo is improper because the reference is nonanalogous art per *In re Clay*." This argument is not persuasive because *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1739-40, 82 USPQ2d 1385, 1395 (2007) explains:

> When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, §103 likely bars its patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill. *Sakraida* [*v. AG Pro, Inc.*, 425 U.S. 273, 189 USPQ 449 (1976)] and *Anderson's-Black Rock*[, *Inc. v. Pavement Salvage Co.*, 396 U.S. 57, 163 USPQ 673 (1969)] are illustrative – a court must ask whether the improvement is more than the predictable use of prior art elements according to their established functions.

Here, a person of ordinary skill in the art would have been motivated to make such a modification so that the decryption key can only be accessed (decrypted in this case) by the set top box (using the set top box specific private key) in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Appellant argues, "with the teaching of Spies, the recited 'first logical unit' does not decrypt the accessed encrypted signal, and further does not decrypt the accessed encrypted signal using the recited 'first decryption key.'" This argument is not persuasive because Spies discloses that the key used to decrypt the encrypted content is transmitted from the IC card (Figure 7, 50)(second logical circuit) to the processor (Figure 7, 150)(first logical circuit) to decrypt the encrypted video signal (Col. 13, lines 2-8).

Appellant argues, "Spies fails to teach or fairly suggest the recited limitations of encrypting a decryption key, transferring the encrypted encryption key to another logical unit, and decrypting the encrypted decryption key." Examiner has never alleged Spies to teach the above mentioned claim limitation, but instead has stated that Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card

is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted decryption key can only be decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Appellant argues, "Deo fails to remedy this deficiency of Spies as Deo fails to teach of fairly suggest use of the digital certificate exchange technique for uses other than certificate exchange." This argument is not persuasive because Appellant has not considered the cited portions of Deo along with the cited motivation to modify the system of Spies in the manner suggested by the rejections (as discussed above).

Appellant argues, "While Spies may teach that cryptographic service providers (CSPs) can be changed or updated, Spies does not teach a method or system for such updates. In particular, Spies teaches such CSPs are 'preferably...stored in ROM (read only memory)' (column 11 lines 64-66). Appellants respectfully assert that one of ordinary skill in the art would understand that changing software stored in a ROM requires physical replacement of the ROM device." This argument is not persuasive because Spies discloses that the cryptographic service providers stored within the IC cards (Col. 11, lines 47-55) are changing or updating the one or more DLLs that make up the cryptographic service providers (Col. 11, line 64- Col. 12, line 3). Therefore, it is clear from this section of Spies that there is a clear intention to "change or

update" the cryptographic server providers within the IC cards, which meets the claim limitation despite where Spies discloses that these cryptographic service providers are "preferably" (i.e. optionally) stored.

Applicant's argues that a third piece of art, which is not cited, has been introduced to reject claim 6. This is simply not the case. Page 7 of the Office Action mailed on 01 September 2006, shows that claims 1 and 3-7 are rejection under 103(a) as being unpatentable over Spies, in view of Deo. The actual rejection of claim 6 is on page 10 of that same Office Action, with no mention of any additional art. Spies is the only piece of prior art even mentioned with respect to the rejection of claim 6. Prior to the Office Action mailed on 01 September 2006, it was determined that the "changing or updating" of the cryptographic service providers (as discussed above) in Spies met the limitations of "replacing a computer control program stored in a second portion of local memory at said first logical circuit with a new computer control program. Appellant has not challenged this rejection.

Appellant argues that Spies does not disclose "wherein said digital signal is substantially compliant with the Motion Pictures Experts Group (MPEG) format...While Spies may teach the 'video content can be TV broadcasts' as stated in the rejection. Appellants respectfully assert that the recited signal is not limited to 'TV broadcasts' or even to video." This argument is not persuasive because Spies discloses video content delivered to the settop box/video player (Col. 2, lines 26-38) can be delivered via satellite TV networks (Col. 1, line 21) or DVDs (Col. 1, line 24). It was the position of the Examiner, that MPEG format was inherent to **video** signals distributed over satellite TV networks and DVDs.

Appellant argues, "it is well known that compact disc (CD) audio is digital; however, it is generally not encoded in MPEG." Appellant's argument is not relevant to the claims, nor is it relevant to the rejection of claim 7. Examiner has stated that Spies meets the limitation of claim 7 because the video content in Spies is distributed over satellite TV networks (Col. 1, line 21) or DVDs (Col. 1, line 24), which inherently use MPEG format.

Appellant argues, "The rejection cites, but does not rely on, Walkinson, 'The MPEG Handbook,' 2004, Focal Press, Second Edition, Pages 366-381, 389-394 ('MPEG'). Appellants are confused by the rejection's treatment of this reference. MPEG shows a publication date of 2004, which is significantly later than the priority date of the present application (2001). Even *arguendo*, using the earliest copyright date of 2001 listed for the non-cited first edition of MPEG, MPEG does not appear to qualify as § 102(b) prior art, as MPEG was published less than one year prior to the priority date of the present application (2001)." This argument is not persuasive because the Examiner has never relied on MPEG as prior art in the rejection of claim 7. MPEG was introduced by the Examiner in the Office Action mailed 01 September 2006, as rebuttal evidence and in support of Examiner's initial position that the MPEG format was inherent to video distribution over satellite TV networks and DVDs. In Appellant's remarks filed 17 July 2006, Appellant formally challenged the Examiner's position of inherency by stating, "Applicant's respectfully note that MPEG-2 is not used for all satellite television. For example, MPEG-2 is not used for analog satellite television transmission." Examiner introduced MPEG in the Office Action mailed 01 September 2006, to show that in video content distributed over satellite networks and encoded on DVDs is in one format, and one format only, **MPEG** (See the previously presented evidence document MPEG Handbook, pages 368-369 & 390, included as

an appendix). Therefore, because Spies discloses that the video is distributed via satellite networks or DVDs, the limitations involving the MPEG format are met.

Appellant argues, "Spies is directed to 'purchase and delivery of video content programs over various distribution media' (Abstract, emphasis added). Appellants do not find Spies to exclude non-digital distribution." This argument is not persuasive because since Spies **does specifically disclose** that the video content distributed in the system of Spies **could be distributed via satellite TV networks or DVDs**, the limitations are met despite any other possible distribution means that may be cited.

Appellant argues, "Spies teaches, '[v]ideo content programs are commonly supplied to viewers in many different forms, including theater films, video cassettes, TV cable and broadcast systems, game CDs, and on-line networks' (column 1 lines 14-17). Appellants respectfully assert that it is well known that the taught 'theater films (and) video cassettes' are non-digital media. Appellants respectfully assert that it is well known that the taught 'TV cable and broadcast systems' may be non-digital, and in fact the majority of such systems, including over-the-air broadcast television, are non-digital." This argument is not persuasive because since Spies **does specifically disclose** that the video content distributed in the system of Spies **could be distributed via satellite TV networks or DVDs**, the limitations are met despite any other possible distribution means that may be cited.

Applicant attempt to disqualify any statements of inherency by alleging that "Audio Video Interleave ('AVI') encoding is widely used in the taught 'on-line networks'," is not persuasive because although AVI formatting may be use in **on-line networks**, it is **not** used in

satellite networks or DVDs. Therefore, the teaching of MPEG encoding is still inherent to **satellite networks and DVDs**.

In response to applicant's argument that Spies teaches away from embodiments of the present invention with respect to Diffie-Hellman, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

Appellant argues, "Spies teaches, '[t]he view computing unit 60 is not permitted, however, to read the decryption capabilities' (column 9, lines 25-26, emphasis added) and 'the individual packet keys are never made available to the viewer computing unit...' (column 10, lines 46-47, emphasis added). Thus, in accordance with the teaching of Spies, the recited 'first logical unit' does not decrypt the accessed encrypted signal, and further does not derypt the accessed encrypted signal using the recited 'first decryption key'." This argument is not persuasive because Spies discloses that the key used to decrypt the encrypted content is transmitted from the IC card (Figure 7, 50)(second logical circuit) to the processor (Figure 7, 150)(first logical circuit) to decrypt the encrypted video signal (Col. 13, lines 2-8). Therefore, the processor of Spies does in fact decrypt the encrypted video signal using the "decryption key". The fact that the individual packet keys are not available to settop box of Spies, which are not directly used to decrypt the encrypted video signal, is not relevant to the suggested modification of Spies, in view of Deo, further in view of Schneier, which suggests that it would have been

obvious to one of ordinary skill in the art at the time the invention was made to use the Diffie-Hellman algorithm for public key exchange in the secure video content delivery system of Spies because Diffie-Hellman gets its security from the difficulty of calculating discrete logarithms in a finite field as taught by Schneier (Page 513).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Benjamin E. Lanier
Examiner AU 2132
Granted Temporary Full Signatory Authority

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Gilberto Barron
SPE AU 2132

Matthew Smithers

/Matthew Smithers/
Primary Examiner AU 2137